

# **EXHIBIT 88**



**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,  
Plaintiffs,**

**v.**

**BRAD RAFFENSPERGER, ET AL.,  
Defendants.**

**DECLARATION OF  
J. ALEX HALDERMAN**

**Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. I have reviewed the expert disclosures prepared by Dr. Juan Gilbert and Dr. Benjamin Adida for State Defendants. Neither Dr. Gilbert nor Dr. Adida offers any rebuttal to the numerous, critical vulnerabilities in Georgia's BMDs that I described in my July 1, 2021 expert report. Dr. Adida did not respond to my report at all; State Defendants reissued prior declarations from him previously provided in this litigation. Neither of them disputes the presence of any of the serious

what Dr. Gilbert acknowledges those ballots would suggest about the reliability of the election.

22. That State Defendants may not know this information is consistent with gaps in other important election data that Georgia counties report to the Secretary of State. State Defendants recently produced electronic data (election projects) that I understand were required to be returned to them by counties after the November 2020 and January 2021 elections. In both elections, a large fraction of counties failed to return any data, returned the wrong data, or omitted data necessary for assessing the security and integrity of the result, such as election databases or ballot images. More than six months after these elections, the Secretary of State has not been able to assemble these electronic records and has not indicated any effort or willingness to do so. Yet the only way that State Defendants could use the number of spoiled ballots as a defense against BMD-based cheating would be if the poll workers accurately tracked it, counties accurately aggregated it, and the Secretary's Office received such data from across the state before the election result was determined. Even then, it is unlikely that the Secretary would be prepared to react by *rerunning the election* if the number of spoiled ballots exceeded the number predicted in an outcome-changing attack.

23. Given the ineffectiveness of such defenses and the critical security problems in Georgia’s BMDs, I (like Dr. Appel) recommend that BMDs be reserved for voters who need or request them, as is the case in most states. Dr. Gilbert responds by claiming, without evidence, that “[d]isabled voters are even less likely to identify an error on their printed ballot” (§ 14). I am unaware of any study that supports this sweeping indictment of voters with disabilities, which encompasses a vast array of disabilities that would not impact the ability of the voter to identify an error on their printed ballot in any way. He also contends that blind voters cannot detect errors on their ballot at all, but this is not true. Many blind voters use assistive technology to read printed text and likely could do so to verify their ballots. Moreover, only some voters who need BMDs are blind. For instance, those with motor impairments that prevent them from marking a ballot by hand would not necessarily have any greater difficulty verifying the printed text than any other voter. In any case, if BMDs are used primarily by voters with disabilities (as in most jurisdictions that use BMDs), they will represent a *much* smaller target,<sup>7</sup> and an

---

<sup>7</sup> Although Dr. Gilbert cites a figure that would imply that 10% of Georgians who voted in 2020 were disabled, data from Maryland, where BMDs are available upon request, suggests that only about 1.8% of voters would request to use BMDs if they were offered a hand-marked ballot first. (*Halderman decl.*, Aug. 19, 2020, Dkt. 785-2 at 49.) Dr. Gilbert’s citation to the number of all Georgia voters with disabilities is highly misleading since, again, very few of those voters would be

outcome-changing attack on any given election will be detectable with a much lower rate of voter error detection than when all in-person voters use BMDs as they do in Georgia today. This in turn creates a strong disincentive for bad actors to attempt hacking an election (the risk likely is not worth the reward when the outcome is highly unlikely to be changed), which means individual votes would be less likely to be altered by hacking.

24. In his only direct response to my expert report, Dr. Gilbert states that he is not aware that I have “provided equipment marred by ‘undetectable’ hacks to any other independent researcher” (§ 15).<sup>8</sup> This is a curious and ironic criticism coming from Dr. Gilbert, since he evidently chose not to evaluate my findings through an examination of the voting equipment himself, which he does not explain. Moreover, Dr. Gilbert misreads my report. It does not claim that malicious software infecting a BMD would be undiscoverable by any possible means. If an individual BMD is

---

unable to vote on a hand-marked paper ballot, consistent with the number reported in Maryland.

<sup>8</sup> Dr. Gilbert ignores that, as I understand it, State Defendants have objected to my report and the underlying work being shared with third parties (except Dominion), including other independent researchers, with whom I am eager to share my work for review. I am confident in my findings and believe they should be shared promptly with appropriate election security researchers and officials in an effort to mitigate the critical vulnerabilities in Georgia’s voting equipment that I describe. I invite Dr. Gilbert to join me in seeking State Defendants’ consent to do that.

*known* to contain malware, there will likely be some level of detailed forensic scrutiny that can detect where the malware is, perhaps requiring months of expert analysis per machine at extraordinary expense. It would be completely infeasible to perform this level of analysis on every machine before every election, much less between an election and the deadline for certification of its results. (And after manipulating ballots, malware could remove all traces of its presence from a machine, defeating any possible post-election examination of the device.) What my report shows is that vote-stealing malware of the type I have constructed would not be detected by any of the defenses that State Defendants purport to practice. I describe in detail how such malware would defeat QR code authentication, logic and accuracy testing, on-screen hash validation, and external APK validation (as was used by Pro V&V after the November election). Dr. Gilbert offers no rebuttal to these findings. He does not dispute them or even address them.

25. Moreover, there is already an example of an “undetectable” attack entered into testimony: exploitation of the Drupal vulnerability discovered by Logan Lamb in the Center for Election Systems server. As Lamb attested, the developers of the primary tool for detecting this vulnerability stated that “[n]either [the defensive tool] nor an expert can guarantee a website has *not* been compromised. They can only

components of Georgia’s voting system. As I have previously pointed out, many election system components that could have been compromised in this way are still in use in Georgia today, where they provide a means by which attackers could spread vote-stealing malware to the BMDs.

27. Rather than address the many threats to Georgia’s voting system, Dr. Gilbert persists in drawing illogical comparisons between BMDs and hand-marked paper ballots. For instance, he questions why Plaintiffs have presented no research “regarding voters’ proclivity to review [hand-marked paper ballots] to ensure their ballots are marked and will count as intended” (§ 8). Much like Dr. Gilbert’s earlier testimony that “[i]n essence, a BMD is nothing more than an ink pen,”<sup>12</sup> one does not need expertise in election security to find fault with this reasoning. Preventing voters from making accidental mistakes is a completely different problem from preventing their selections from being deliberately and systematically changed by an attacker who has compromised the BMDs. There is abundant evidence that voters do sometimes make errors whether filling out a ballot by hand or by machine. Bad ballot design exacerbates this problem with both voting modalities, but following ballot design best practices can greatly reduce it. Both

---

<sup>12</sup> *Gilbert decl.*, Dkt. No. 658-3 at 60.

BMDs and scanners that count hand-marked ballots can also be configured to reject overvotes and to warn voters about undervotes, the most common kinds of voter errors. Moreover, unlike older technologies for counting hand-marked ballots, the scanners used in Georgia (when properly configured) can detect improperly or incompletely marked bubbles and present them to human operators to adjudicate whether the marks should count as votes. Election officials can use all of these options to help protect voters from their own mistakes, but none of them offers protection against a BMD that deliberately changes the selections printed on a voter's ballot (or those encoded in the ballot barcode). The central problem with Georgia's highly vulnerable BMD system—that attackers can change all records of the voter's intent without being detected by election officials—has no parallel in a hand-marked paper ballot system.

28. Dr. Gilbert concludes as he started, with vague and sweeping generalities. “Simply put, BMD elections systems are no more insecure than [hand-marked] systems” (§ 16). It is unclear whether he is claiming that *all* BMD systems are at least as secure as all hand-marked systems or merely that some specific BMD system (such as the one he recently developed himself to address some of the reliability problems that exist with Georgia's BMDs) is at least as secure as some hand-marked system, but this is of little consequence. The only BMD system that is



BMDs for voters who need or request them. Absent security improvements such as this, it is my opinion that Georgia's voting system does not satisfy accepted security standards. Neither Dr. Gilbert nor Dr. Adida offers a contrary opinion in their respective declarations, instead ignoring the critical issue of whether the *voting system used in Georgia*—which neither claims to have examined—reliably protects the right to vote for individual Georgia voters.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 2<sup>nd</sup> day of August, 2021 in Rushland, Pennsylvania.



---

J. ALEX HALDERMAN